AGENDA

Safety Share
Who is Cleco?
CIP-005-3, R5
How
What
SAFETY SHARE
Statistics: General

• Customers: approx. 279,000 retail customers across Louisiana
• Non-contiguous transmission and service area
• Generation:
  2,560 MW regulated
  775 MW un-regulated
  691 MW jointly owned
• Transmission Lines:
  approx. 1,300 miles (primarily 138 & 230 KV)
• Distribution Lines:
  approx. 11,500 miles
Cleco Service Territory
SPP

- NERC Regional Entity (RE) is SPP
- SPP acts as Cleco’s Reliability Coordinator
- Member, Southwest Power Pool (SPP)

- Cleco is NOT a member of the SPP RTO
- Cleco is a Transmission Provider under its own FERC approved OATT
CIP-005, R3

• How did we approach?

Industrial Defender’s SEM (Security Event Monitor)

Industrial Defender and EMS vendor worked together to integrate SEM into EMS package.

Logs, monitors, and alerts for events on Cyber Assets within ESP
Hardware/Software

- **Hardware**
  - SEMs located at Primary & Backup facilities

- **Software**
  - Each CA or CCA host sends log to each SEM
Network

HIDS: Host Intrusion Detection System
RIDS: Remote Intrusion Detection System
Logging

- SEM configured to log events for:
  - All successful and unsuccessful logins
  - Privileged user activity
  - Access to shared accounts

- Logs reviewed weekly by CTO Support
Example

Interactive Login Events on **guard-esp** from December 10th - 27th:

---

Dec 10 10:25:23 **000.111.222.33** time=10:25:23 devname=guard-esp device_id=serial number log_id=0104041990 type=event subtype=admin pri=information fwver=040004 vd=root user="account" ui=https(000.111.222.33) action=login status=success reason=none profile="super_admin" msg="Administrator account logged in successfully from https(000.111.222.33)"

Dec 10 10:34:39 **000.111.222.33** time=10:34:39 devname=guard-esp device_id=serial number log_id=0104041990 type=event subtype=admin pri=information fwver=040004 vd=root user="account" ui=https(000.111.222.33) action=login status=success reason=none profile="super_admin" msg="Administrator account logged in successfully from https(000.111.222.33)"

Dec 10 15:58:17 **000.111.222.33** time=15:58:17 devname=guard-esp device_id=serial number log_id=0104041990 type=event subtype=admin pri=information fwver=040004 vd=root user="account" ui=https(000.111.222.33) action=login status=success reason=none profile="super_admin" msg="Administrator account logged in successfully from https(000.111.222.33)"

Dec 11 07:46:23 **000.111.222.33** time=07:46:23 devname=guard-esp device_id=serial number log_id=0104041990 type=event subtype=admin pri=information fwver=040004 vd=root user="account" ui=https(000.111.222.33) action=login status=success reason=none profile="super_admin" msg="Administrator account logged in successfully from https(000.111.222.33)"

Dec 27 09:35:26 **000.111.222.33** time=09:35:26 devname=guard-esp device_id=serial number log_id=0104041990 type=event subtype=admin pri=information fwver=040004 vd=root user="account" ui=https(000.111.222.33) action=login status=success reason=none profile="super_admin" msg="Administrator account logged in successfully from https(000.111.222.33)"

---

Note: Bold items have been altered for security.
Alerts

• Automatic alerts for unauthorized access attempts:
  – Three failed login attempts in one minute
Alarm

Edit Metric Template

Template Settings
- Host Template Group: ID Guard 310B
- Name: Authentication: Login fail event

Email Sent To
- Send To: callout-pager

Alerts
- Immediate Alert Priority: P6
- Enable Threshold Alerts:
  - Hi Alarm: 15.0 failures/min, Priority P1, Email: Yes
  - Hi Warn: 3.0 failures/min, Priority P2, Email: Yes
  - Normal State

Comments

Save
From: ctocadmin@cleco.com [ctocadmin@cleco.com]
Sent: Thursday, February 21, 2013 11:28 AM
To: CTOCSupport
Subject: Alert from Industrial Defender SEM Console

Feb 21, 2013 11:28:16 AM 0 Windows event logs: Failure audit dominator Rtn-to-Norm
Investigate

• When alert is received:
  – CTOC Support will investigate the cause of the event
  – Determine if malicious or accidental
    • If malicious or cannot be proven accidental, report per Incident Reporting and Response procedure
Louis C. Guidry, P.E.
Manager NERC Compliance & Training
Work 318-484-7495
Cell 318-308-9121
louis.guidry@cleco.com
2013 SPP CIP
Compliance Workshop

CIP-005 R3: Monitoring Electronic Access

May 21, 2013
Agenda

• System Overview
• Westar’s Approach to CIP-005 R3
  – CCAs, PCAs, and EACMs
  – Other EACMs [CIP-005 R1.5]
  – PACSs [CIP-006 R2.2]
• Recommendations
• CIP Version 5 Plans
  – Integrated Security Monitoring Approach
  – Enterprise Security Incident and Event Monitor
• Questions
Westar System Overview

- Statistics
  - 2,400 Employees
  - 700,000 Customers
  - 3,300 Miles of Transmission
  - 7100 MW of Total Generation

Generation Capacity Mix

- Coal Fired - 3429MW
- Gas/Oil (Steam) - 1059MW
- Gas/Oil (CT/CC/IC) - 1772MW
- Wind - 695MW
- Nuclear - 545MW
Westar System Overview
• EMS Cyber Assets– Automated Approach
  – TDi’s ConsoleWorks monitors electronic access into the EMS ESPs including, but not limited to following devices:
    • EMS Communication Servers
    • VPN Devices
    • ConsoleWorks Appliances
  – Provides automated logging, monitoring, and alerting of events on in-scope Cyber Assets.
  – Primary and Secondary ConsoleWorks
    • Provides redundancy and failover capability
    • Syslogs pushed to ConsoleWorks
    • Alert notifications via page
CIP-005 R3 - Westar’s Approach

<table>
<thead>
<tr>
<th>Event Occurrences</th>
<th>Log Data</th>
<th>Severity</th>
<th>Action</th>
<th>First Occurred</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OP_WIN_515_SECURITY (2)</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:19</td>
<td>A trusted login process has registered with the Local Security Authority.</td>
</tr>
<tr>
<td>OP_WIN_540_SECURITY (1)</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:18</td>
<td>Successful Network Login.</td>
</tr>
<tr>
<td>OP_WIN_540_SECURITY (1)</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:15</td>
<td>Successful Network Login.</td>
</tr>
<tr>
<td>OP_WIN_540_SECURITY (1)</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:19</td>
<td>Successful Network Login.</td>
</tr>
<tr>
<td>OP_WIN_576_SECURITY</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:19</td>
<td>Special privileges assigned to new logins.</td>
</tr>
<tr>
<td>OP_WIN_576_SECURITY</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:19</td>
<td>Special privileges assigned to new logins.</td>
</tr>
<tr>
<td>OP_WIN_576_SECURITY</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:20</td>
<td>Special privileges assigned to new logins.</td>
</tr>
<tr>
<td>OP_WIN_576_SECURITY</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:21</td>
<td>Special privileges assigned to new logins.</td>
</tr>
<tr>
<td>OP_WIN_576_SECURITY</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:21</td>
<td>Special privileges assigned to new logins.</td>
</tr>
<tr>
<td>OP_WIN_576_SECURITY</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:21</td>
<td>Special privileges assigned to new logins.</td>
</tr>
<tr>
<td>OP_WIN_576_SECURITY</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:21</td>
<td>Special privileges assigned to new logins.</td>
</tr>
<tr>
<td>OP_WIN_576_SECURITY</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:21</td>
<td>Special privileges assigned to new logins.</td>
</tr>
<tr>
<td>OP_WIN_576_SECURITY</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:21</td>
<td>Special privileges assigned to new logins.</td>
</tr>
<tr>
<td>UNK_CE_FAM_SECURITY</td>
<td></td>
<td></td>
<td></td>
<td>2013/04/24 10:19</td>
<td>Failed module login tested.</td>
</tr>
</tbody>
</table>

---

CIP-005 R3: MONITORING ELECTRONIC ACCESS

Westar Energy
CIP-005 R3 - Westar’s Approach
CIP-005 R3 - Westar’s Approach

- **EACM Cyber Assets – Hybrid Approach**
  - Splunk monitors electronic access into the ESPs
    - Firewall syslogs are sent to a centralized monitoring console loaded with Splunk for indexing,
    - Custom scripts execute hourly monitoring for alerts,
    - Script then emails the reports to IT Security Analyst for review.
  - Primary and Secondary Logging Consoles
    - Provides redundancy and failover capability
CIP-005 R3 - Westar’s Approach
CIP-005 R3 - Westar’s Approach

- PACS Cyber Assets – Manual Approach
  - Physical Access Controls System (PACS) Monitoring
    - PACS electronically monitors 24x7 using its own logging mechanism.
    - PACS application is unable to automatically alert on attempted or actual unauthorized access events.
  - TFE in-place to accommodate compensating controls
    - Implemented a process where a custom script is used to extract and capture systems events.
    - Monthly review of attempted or actual unauthorized access events using an exception tracking log.
Recommendations

• Best Practices
  – Provide examples of an alert generated for a failed login.
  – Make certain each alert has a documented response.
  – Describe in your procedures the different types of events that will trigger an alert.

• Evidence
  – Documented procedure,
  – Attempted or actual unauthorized access logs, and
  – Examples of automated or manual alerts.
CIP Version 5 Plans

- Integrated Security Monitoring Approach

Diagram:
- Security Monitoring
  - Information Technology (IT)
  - Operational Technology (OT)
  - EMS
  - Substation Protection and Controls
  - Plant Instrument and Controls (I&C)
CIP Version 5 Plans

• Enterprise Security Incident and Event Monitor
  – Automated detection for all known or suspected malicious communications for both inbound and outbound communications from the Electronic Access Points.
  – Automated event logging and alerting from all NERC CIP BES Cyber Systems and/or Cyber Assets.
    • Log parsing, normalization, correlation, analysis, and alerting.
    • Application logs, System logs, Network device logs, Network flow data, Control systems
Questions?

Eric Ervin
Manager, NERC CIP
(785) 575-1626
eric.ervin@westarenergy.com